A REVIEW ON CYBER SECURITYAND ITS INTERVENTIONS STRATEGIES IN INDIA

MOHIT BAJPAI, TAKSHIMA GOYAL, SHRUTI JAIN

[1]Assistant Professor,[2]Student, B.Tech. 1st Year[3]Student, B.Tech. 1st Year
[1]Department of ECE,
[1]Poornima Institute of Engineering & Technology, Sitapura, Jaipur, Rajasthan, India [302022]

Abstract:Technology of today has advanced. One can communicate with another person across the world easily. It is also helpful in medical field. But today cyber-crime is increasing all over the world especially in India. Information sharing, data out, malware, computer viruses, surveillance, etc. are some of the major problems which gives the growth to cyber-crime in India. So, to stop the cyber-crime, one should aware about the cyber security. Today some serious games are developed for graduate engineers to learn cyber security. In this paper, we learn about the need of cyber security in India in today's scenario, how to overcome these cyber-crimes and protect the data of public from hacking and other cyber-crimes. In this paper, we also get to know about the cyber security to protect the ICT infrastructure which is like the mother of all the technology infrastructure.

***IndexTerms*–Cyber-crime, Cyber security, Malware, ICT Infrastructure, Hacking, Computer virus.**

I. INTRODUCTION

WHAT IS CYBER CRIME?

Now-a-days, cyber-crime is one of the major problems regarding security. Most of our daily life works are based on internet services. Internet provide us various opportunity in all types of fields. Internet helps us growing business, organizations, education system, e-banking. It is used as greatest exchange source of information and also used for communication system. We can say that our life is becoming more dependent on these technologies. Even the children use internet for the projects and school works. There are many games which are based on knowledge and education. Even in schools, the teaching method has been changed now. It is transformed from classroom lecture into digital teaching. But apart from these, it results into cyber-crimes. Insecurity of data, information regarding bank account details is become biggest issue for the world. It is become serious problem for the information industry. Internet is used to manipulate details of users. Important data is stolen by the hackers using internet. Cyber targeting various organizations, public sectors. These crime does not need much investment as compare to other crimes and can be done from various locations easily. [1]

The threats to cyber security are growing at vast rate. Cyber security gained momentum in the 1990's with the advancement in science and technology. Crimes grown up by 60% every year. In year 2011, 2070 cases and 3500 in 2012 reported in India. As per reports from National Crime Records Bureau (NCRB), Maharashtra reports 561 cases, Andhra Pradesh 454 cases, Karnataka 437 cases in the year 2012 crimes which are done by age group of 18 to 30. Haryana registered 3 cases in 2011 but 116 in the year 2012.

WHAT IS CYBER SECURITY?

Cyber security means being protected from unwanted activities in computer which leads to the cyber-crimes. It is the program, practice, or we can say that it is the way to stop the cyber-crimes. It protects the people's personal data, information, etc. from the eye of hackers and unauthorized access.

BACKGROUND OF CYBER SECURITY INFRASTRUCTURES –

Cyber security infrastructure is very important in the field of science and technology. It is the backbone for the society for the development. It plays the vital role in the growth of technology and security in the society. Interconnection of these infrastructure in large and broad area leads to information sharing, data out and other threats which directly leads to the cyber-crimes. Conversation between countries becomes blurred due to lack of trust and privacy. It becomes the framework for the cyber-crimes in India.

THREATS TO ICT INFRASTRUCTURE –

Means to destroy, harm to a system or overall organizations. The attack against an information can be done with both physical implements like hammer, backhoe and cyber based hacking tools. All these four types of threats involve the malicious use of the information infrastructure either as a target or as a tool (Dunn, 2006).[2]

1. Bombing an electrical grid, severing a telecom with a backhoe, smashing a server with hammer.
2. Electronic components can be destabilized by the use of electromagnetic pulse and radio frequency weapons.
3. SCADA system are hacked to control municipal sewage.
4. Critical government network are hacked.

MANAGEMENT OF CYBER SECURIY RISKS –

Management of cyber security depends upon three factors –

1. Threats
2. Vulnerabilities
3. Impacts

1. **THREATS** – People who involve in cyber-attacks falls or divided in five categories –

(a) Criminal
(b) Spies
(c) Nation-state warriors
(d) Hacktivists
(e) Terrorists

2. VULNERABILITIES – Cyber security is generally an arm race between attackers and defenders. ICT infrastructure has complexities. There are some weak points on which attacker attack on them and defender try to strong them or remove them. But there are three problems we generally face –

(a) International act by insider which access our system
(b) Malicious virus inside our system
(c) Unknown vulnerability

3. IMPACTS – Cyber-attacks has a major impact on society and country. Hackers hack the system which leads to the information sharing and danger to privacy through which other can access our system. If attackers attack on the industries data then it leads to the destruction of the machines, pumps, generators, etc. It also has the worst impact on the economy of the country. Some serious games are developed now-a-days which give the growth of crime in children. Due to which they come into depression and committed suicide which is very wrong.[3]

NEED FOR CYBER SECURITY IN INDIA –

Most of today's transactions are online. Over 1700 cases of fraud related to debit/credit card and internet banking with the extent of losses touching Rs. 71.48 crore were reported in 2017. The following graph **(Figure1)** shoes India payment type in the year 2012 according to which is online transaction is more. [4]

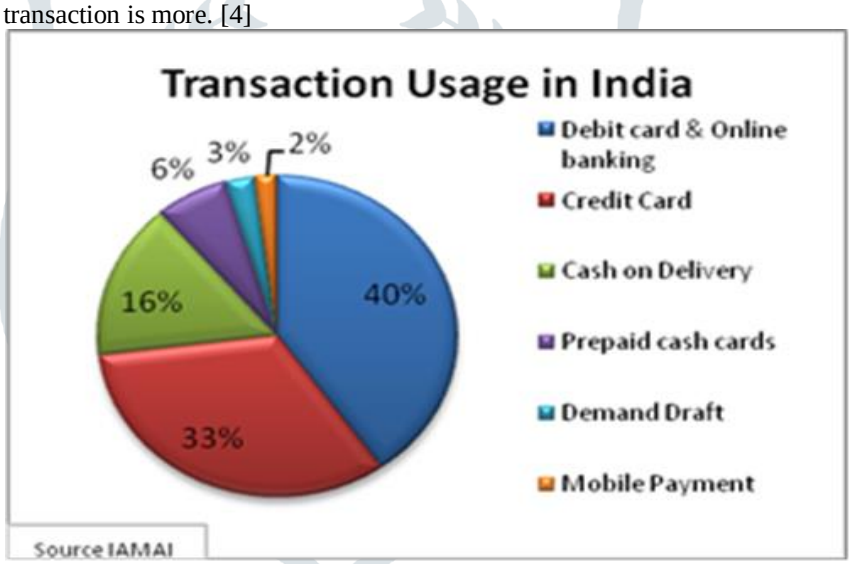


FIGURE 1: Percentage of usage of different online payment methods in India

ASPECTS OR TYPES OF CYBER SECURITY –

1. **NETWORK SECURITY –** It is common type of cyber security from one local user to other computer users through network. As we know data is provided to only some authorized users, so it is easy for hackers to stole data by typing correct data name and password. So here security of network is important so that the work of network go smooth without any disturbance.

2.DATA SECURITY –Data security is another important category of cyber safety. It is related to security of data which is stored in computers from threat through antivirus and firewalls.

3. **SYSTEM SECURITY –** It is another important type of cyber security. In this some malicious programs destroyed the computer system. Some malicious programs are viruses, rabbis, trojan horses, bugs, etc. hackers candamage the system by using them. So, here security of system is very much important.

TYPES *OF CYBER ATTACKS –*

1. ACTIVE ATTACK - In this attack hackers try to make changes in the data. It attempts to alter system resources or effect their operations.

2.DENIAL OF SERVICE – Users are disadvantaged for the access use of network and its resources. It also prevents normal use of communication facilities.

3. PASSIVE ATTACK – In this attack attacker obtain the information is being transmitted without being damaged to the system resources.

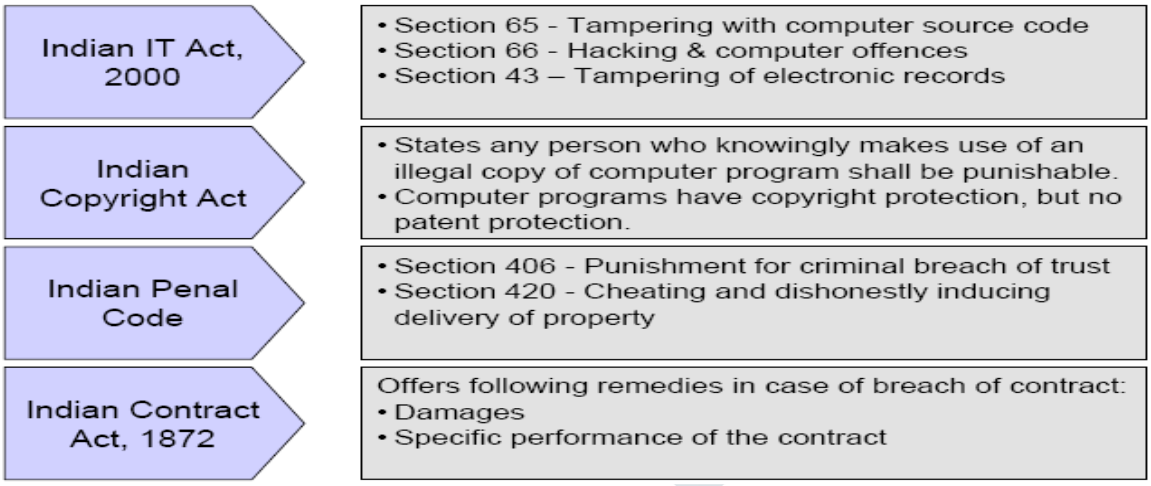
4. TRAFFIC ANALYSIS – It is a special type of attack in which attacker capture the message and try to solve it to take information while communication.
5. PASSWORD ATTACK- This is the most common attack in which access to a person's password is obtained by looking around the person's desk.
6. MALWARE ATTACK – Malicious software [5]

PREVENTIONS METHODS FOR CYBER CRIME –

Cyber-crimes can be stopped easily stopped by some technical advice and common sense. Cyber attackers or hackers always try to find easy way to give the growth to cyber-crime.We can make it tough by using advanced technical and security features in computer device. Cyber-crimes can be stopped by having the education and advanced security -features about cyber security. It should be safe for old age and children from all these crimes happening in India. Computer security is designed in such a way which protect a computer from accidental or intentional theft, unauthorized access or manipulation.
It is always said that precautions are better than cure. So, some of the precautions are as follows –

1. Never share passwords to others even to your close ones and never write it anywhere.
2. Your password should be different from others means it should not contain your name, mobile no., birth dates, etc. In short, password does not contain your personal detail.
3. Try to avoid sharing your picture with strangers while chatting with them.
4. Not share your bank details on any other site.
5. Don't see someone's personal detail on any website.
6. When you install any app, first verify it by play-store.
7. Deny permissions who ask for access your photos or contacts.
8. Use of computer firewalls is beneficial.
9. Use updated and advanced antivirus for both software and hardware.
10. Don't click on the link of unknown origin, first verify it.

CYBER SECURITY INITIATIVES IN INDIA –



(Source: Saravade, 2007)
Figure 2: Legal Framework to support Cyber Security in India

1. INDIAN GOVERNMENT INITIATIVES (figure 2) –
(a) Cyber Security Research and Development Centre of India (CSRDSI)
(b) Cyber Crimes Investigation Centre of India
(c) National Intelligence Grid (NATGRID)
(d) National Critical Information Infrastructure Protection Centre (NCIPC) of India
(e) National Cyber Security Database of India (NCSDI)
2. OTHER INDIAN GOVERNMENT INITIATIVES FOR EDUCATION ON CYBER SECURITY –
(a) Information Security Awareness
(b) Information Security Education and Awareness project
(c) National Initiative for Cyber Education (NICE)
3. TOP COLLEGES WHICH OFFER CYBER SECURITY COURSE IN INDIA –
(a) Institute of Management and Technology – Ghaziabad, Uttar Pradesh
(b) Amrita School of Technology – Coimbatore, Tamil Nadu
(c) Amity University – Noida, Uttar Pradesh
(d) Faridabad Institute of Management Studies – Faridabad, Haryana
(e) Institute of Management Technology – Ghaziabad, Uttar Pradesh
(f) Sarvodaya Law College – Bangalore, Karnataka

LATEST TECHNOLOGIES USED IN CYBER SECURITY –

1. CRYPTOGRAPHY – It is the study and practice of techniques to secure communication in the presence of third party. Construction and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in IS such as data integrity, authentication and non-repudiation.

2. ARTIFICIAL INTELLIGENCE – It allows us to detect threats automatically and combat even without the involvement of human being. It powering our data to stay more secure. AI is totally machine language. It assures for complete error free cyber security services.

3. DATA LOSS PREVENTION – It is a technology such as encryption and tokenization. They can protect data down to field and subfield level, which can benefit in a number of ways:

- Cyber attackers can't monetize data.
- Data can be securely moved across the extended enterprises.
- Provides security regulations for protection of PCI, PII, PHI.

4. CLOUD SECURITY – Cloud security is the protection of data, applications and infrastructures involved in cloud computing. Cloud security provides some preventive protections-

- Can see the current state of security.
- Know immediately about the unusual happens.
- Can respond unexpected events.

IV. RESULTS AND DISCUSSION

India lags far behind when it comes to official cyber security workforce which comprises a small number of experts deployed in various government agencies. It can be concluded from this present study that to defend against cyber-crimes, intrusion detection techniques should be designed, implemented and administrated. The way to protect it for now is for everyone to be smart and to follow preventive measures. India is progressing by implementing proper policies and by implementing well designed laws.

In addition, students should be aware of various options before playing the game about cyber threats and crimes. Cyber-crimes cause damage which results to long term setback to economy.

REFERENCES

[1] Singh Anurag and Singh Brijmohan, 2017, Cyber security Policies for digital India: Challenges and Opportunities, International journal of Computer Sciences and Engineering, Volume-5, 164-168.

[2] Shweta Ghate and Pragyesh Kumar Agarwal, 2017, A literature review on cyber security in Indian context, Journal of computeand information technology, 8(5), 30-36.

[3] K. Jaishankar, 2018, Cyber criminology as an academic Discipline: History, Contribution and impact, International journal of cyber criminology, Volume-12, 1-8.

[4] Yu-Hsien Sung, 2018, Book review of cyber bullying approaches, consequences and interventions, International journal of cyber criminology, Volume-12, 1-9.

[5] Ioannis Agrafiotis, Jason R.C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton, 2017, Ataxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, Journal of cyber security, Volume-10, 1-15.